Lower Bounds for DNF-Refutations of a Relativized Weak Pigeonhole Principle

Albert Atserias
Universitat Politècnica de Catalunya
Barcelona, Spain
atserias@lsi.upc.edu

Moritz Müller
Kurt Gödel Research Center
Vienna, Austria
moritz.mueller@univie.ac.at

Sergi Oliva
Universitat Politècnica de Catalunya
Barcelona, Spain
oliva@lsi.upc.edu

***Abstract*—The relativized weak pigeonhole principle states that if at least $2n$ out of n^2 pigeons fly into n holes, then some hole must be doubly occupied. We prove that every DNF-refutation of the CNF encoding of this principle requires size $2^{(\log n)^{3/2-\epsilon}}$ for every $\epsilon > 0$ and every sufficiently large n. For its proof we need to discuss the existence of unbalanced low-degree bipartite expanders satisfying a certain robustness condition.**

I. Introduction

The pigeonhole principle PHP_n^m expresses the fact that there is no injection from m pigeons into n holes whenever m is bigger than n. As usual, we formulate PHP_n^m as a contradictory CNF in the propositional variables $P_{u,v}$ with u ranging over an m-element set $[m]$ of pigeons and v ranging over an n-element set $[n]$ of holes. The formula has clauses $\neg P_{u,v} \vee \neg P_{u',v}$ for $u, u' \in [m]$ with $u \neq u'$ and $v \in [n]$ forcing different pigeons to fly to different holes, and $\bigvee_{v\in[n]} P_{u,v}$ for $u \in [m]$ forcing every pigeon to fly to some hole. Estimating the refutation-complexity of this set of clauses in various proof systems has a long history in proof complexity dating back to Cook and Reckhow's seminal article [1].

A. Weak pigeonhole principles

One of the most quoted results of propositional proof complexity is that PHP_n^{n+1} does not have short proofs in the standard propositional proof systems that "lack the ability to count". This is confirmed by the seminal results of Haken [2] for resolution, and Ajtai [3] for standard proof systems manipulating formulas of bounded depth (i.e. AC^0-Frege), followed by the great quantitative improvements by Beame, Impagliazzo and Pitassi [4] and Krajíček, Pudlák and Woods [5] on Ajtai's result. In contrast, short polynomial-size proofs exist as soon as the proof systems are allowed formulas that express counting properties, such as arbitrary propositional formulas [6] (i.e. NC^1-Frege), or even threshold formulas of bounded depth (i.e. TC^0-Frege).

From the above, the ability to count looks like an essential ingredient for proving PHP_n^{n+1}. On the other hand, since *approximate counting* is available in AC^0 via explicit polynomial-size formulas [7], one may speculate that *weaker* pigeonhole principles with a much bigger gap between the number of pigeons and the number of holes, such as $PHP_n^{n^2}$ or PHP_n^{2n}, may have polynomial-size bounded-depth proofs. However, this is a notorious 25-year old open problem [8], the main obstacle being that although the known AC^0-formulas for approximate counting are explicit, their *correctness* seems hard to prove. The only known superpolynomial lower bounds are for resolution in the case of $PHP_n^{n^2}$ [9], [10], and for proofs manipulating k-DNFs with $k \leq \epsilon \log n / \log\log n$ for some $\epsilon > 0$ in the case of PHP_n^{2n} [11], [12], [13].

Indeed, for those weaker pigeonhole principles some positive results are known: Paris, Wilkie and Woods [8] proved that $PHP_n^{n^2}$ and PHP_n^{2n} do have quasipolynomial-size bounded-depth proofs, in fact, proofs of barely superpolynomial size (cf. [8], [14]). Their proof does not rely on approximate counting. They prove $PHP_n^{n^2}$ by a clever diagonalization argument and employ an amplification argument to reduce PHP_n^{2n} to $PHP_n^{n^2}$. Analyzing their argument in bounded arithmetic, Krajíček [15], [16] got quasipolynomial-size proofs of the onto-version of PHP_n^{2n} by depth-2 formulas, indeed by k-DNF formulas for k polylogarithmic in n. This was later improved by Maciel, Pitassi and Woods [17] who gave $n^{O((\log n)^2)}$-size such proofs of the original version.

The question whether $PHP_n^{n^2}$ or PHP_n^{2n} have polynomial-size bounded-depth proofs remains open. A positive answer could have consequences for bounded arithmetic [8], and a negative answer could have consequences for our understanding of approximate counting as a computational problem.

B. Our results

Consider the following modified weak pigeonhole principle: if at least $2n$ out of n^2 pigeons fly into n holes,

then some hole must be doubly occupied. To formulate this principle we use additional propositional variables R_u for $u \in [n^2]$ intended to express that pigeon u decides to fly. Formally, the relativized weak pigeonhole principle $PHP_n^{n^2,2n}$ has clauses

$$\neg R_u \vee \neg R_{u'} \vee \neg P_{u,v} \vee \neg P_{u',v}$$

for $u, u' \in [n^2]$ with $u \neq u'$ and $v \in [n]$, and

$$\neg R_u \vee \bigvee_{v\in[n]} P_{u,v}$$

for $u \in [n^2]$, together with a set of *threshold* clauses

$$\mathrm{TH}_{2n}(\bar{R}, \bar{X})$$

in the R_u-variables $\bar{R}$ and some auxiliary variables $\bar{X}$. These threshhold clauses express that at least $2n$ pigeons decide to fly. More precisely, $\mathrm{TH}_{2n}(\bar{R}, \bar{X})$ is a polynomial-size (in n) set of clauses such that for every assignment α to the variables $\bar{R}$ the following holds: there exists an assignment ξ to the auxiliary variables $\bar{X}$ such that $\alpha \cup \xi$ satisfies $\mathrm{TH}_{2n}(\bar{R}, \bar{X})$ if and only if α sets at least $2n$ many variables in $\bar{R}$ to true.

We are ready to state the main result of this paper:

Theorem 1. *For every real $\epsilon > 0$ and every sufficiently large n, every DNF-refutation of $PHP_n^{n^2,2n}$ has size at least $2^{(\log n)^{3/2-\epsilon}}$.*

By a DNF-refutation we mean a proof in a standard proof system that manipulates DNF-formulas. This is, of course, a bounded-depth proof system (depth-2), and is the natural generalization of Resolution to work with DNF-formulas instead of clauses.

C. Proof outline and comparison to previous work

Our proof follows the random restriction method, so successfully used in previous works in propositional proof complexity, with some additional ideas. The typical skeleton of a proof by the random restriction method goes as follows: Assume a short proof of F is given. Apply a random restriction from a suitable distribution in such a way that, with high probability, every formula in the proof simplifies significantly, but the proved formula F remains hard. Finally argue directly that the restricted F cannot have a short proof with such simple formulas.

For an example, suppose PHP_n^{2n} has polynomial-size resolution refutations. For the random restriction we choose an assignment that describes a 1-1 mapping from $n/2$ randomly chosen pigeons onto $n/2$ randomly chosen holes, and leaves all the other variables unset. With these parameters, the restricted PHP_n^{2n} becomes $PHP_{0.5\cdot n}^{1.5\cdot n}$, and each *complex* clause of the proof has been made true with high probability. Now a direct prover-adversary argument shows that a proof of $PHP_{0.5\cdot n}^{1.5\cdot n}$ with non-complex clauses only is impossible.

Trying to apply this argument to DNF-refutations hits several difficulties. First, a random *matching* restriction as above is not likely to simplify an arbitrary DNF formula, even if this formula is small. Indeed, the DNF could be the negation of PHP_n^{2n} itself, and the point of the argument above was precisely that this formula does not simplify much. Here is where our modified version $PHP_n^{n^2,2n}$ enters the picture. By choosing $2n$ out of n^2 pigeons at random and setting all the variables about the other pigeons completely at random, it is very likely that each DNF in the proof simplifies into one all whose terms mention very few of the $2n$ chosen pigeons. This sort of restriction comes inspired by the so-called Dantchev-Riis restrictions [18], and its analysis for our case requires arguments of the type Furst, Saxe, and Sipser introduced in their seminal work on bounded-depth circuits [19].

Continuing with the sketch of the proof, the application of the Dantchev-Riis restriction to $PHP_n^{n^2,2n}$ leaves an instance of PHP_n^{2n}. Unfortunately, a term mentioning very few pigeons need not be short itself, which means that we are not yet at a contradiction with the known lower bounds for PHP_n^{2n} in k-DNF resolution for $k \leq \sqrt{\log n / \log\log n}$ from [12] which were later improved to $k \leq \epsilon \log n / \log\log n$ for some $\epsilon > 0$ [13]. Following the ideas in [20], as adapted to k-DNF proofs in [11], [12], this suggests that we restrict the principle further to a low-degree bipartite expander G (with left vertices $[2n]$ and right vertices $[n]$) to get a short proof of $PHP(G)$. Recall (cf. [20], [21]), this formula is obtained from PHP_n^{2n} by zeroing out all $P_{u,v}$ with (u, v) not an edge of G.

The low-degree condition on G guarantees that whenever a term mentions very few pigeons we can also assume that the term is short, resulting in a k-DNF refutation of $PHP(G)$ for small k. This would seem to open the door to using the methods in [12].

Unfortunately, the sort of bipartite expanders that are needed for the rest of the argument require degree at least as large as $\log n$, leaving k well above the quantity that a direct application of the methods in [12] can afford. Here comes the second main idea in our proof: we use a logarithmic degree expander G, but reduce our problem to proving lower bounds for a related formula $BPHP(G)$ in which the flights of the pigeons along the edges of the graph are encoded in *binary*. This takes us from $k = \Omega(\log n)$ in the unary encoding to $k = O(\log\log n)$ in the binary encoding (at least in

the case that we start with polynomial-size proofs), well below the critical $\sqrt{\log n / \log\log n}$.

Putting all these ideas together into a proper argument requires a fair amount of technical work and this is what the rest of the paper is devoted to. After a few preliminaries in the next section, in Section III we discuss the sort of expander graphs we need, and in Section IV we use them for the proof of the main theorem.

II. Preliminaries

For a natural $n \in \mathbb{N}$, we write $[n] := \{0, \dots, n-1\}$ and $|n| := \lceil \log(n+1) \rceil$. All our logarithms are base 2. Note that, for $n > 0$, the natural $|n|$ is the length of the binary representation of n without leading zeros. For $b \in \mathbb{N}$ we write $\mathrm{bit}(b, n)$ for the $(b+1)$-th least significant bit in the binary representation of n; formally, $\mathrm{bit}(b, n) := \lfloor n/2^b \rfloor \mod 2$. Note that if $b \geq |n|$, then $\mathrm{bit}(b, n) = 0$.

A. Bipartite graphs

Let $G = (U, V, E)$ with $E \subseteq U \times V$ be a bipartite graph. For a vertex $u \in U \cup V$ let $N_G(u)$ be the set of neighbors of u in G and for a set of vertices $A \subseteq U \cup V$, let $N_G(A) := \bigcup_{u \in A} N_G(u)$. A set $M \subseteq E$ is a *matching (in G)* if no two edges in M share an endpoint. Note that matchings M are bijections and thus have an image $\mathrm{Im}(M)$ and a domain $\mathrm{Dom}(M)$.

We say G is a (U, V, d_L, d_R)-graph if for every $u \in U$ we have that $|N_G(u)| \leq d_L$ and for every $v \in V$ we have that $|N_G(v)| \leq d_R$. With such a graph we associate a bijection ϕ_G with $\mathrm{Dom}(\phi_G) \subseteq U \times [d_L]$ such that for every $u \in U$ and every $v \in N_G(u)$ there is (exactly one) $i \in [d_L]$ such that $(u, i) \in \mathrm{Dom}(\phi_G)$ and $\phi_G(u, i) = v$. For a subset $C \subseteq U \cup V$ we let $G \cap C$ denote the subgraph of G induced by the vertices of C; if ϕ_G is associated to G, then $G \cap C$ is a $(U \cap C, V \cap C, d_L, d_R)$-graph and the map associated to $G \cap C$ is (as a set of pairs) $\phi_{G \cap C} := \phi_G \cap ((C \times [d_L]) \times C)$. We also write $G \setminus C$ for $G \cap ((U \cup V) \setminus C)$.

B. Propositional logic

Propositional variables are also called *atoms*. A *literal* is an atom X or its *negation* $\neg X$. A *formula* is built from literals by means of $\vee$ and $\wedge$. Note that we allow the negation symbol only in front of atoms. The *negation* $\neg F$ of a formula F is defined as the formula obtained from F by interchanging $\wedge$ and $\vee$, and replacing every literal by its complementary literal (i.e. X by $\neg X$ and $\neg X$ by X). If Γ is a set of formulas, we write $\bigwedge \Gamma$ for the iterated conjunction of the formulas in Γ; the elements in Γ are the *conjuncts*. Similarly, we write $\bigvee \Gamma$ for the iterated disjunction, and the elements of Γ are the *disjuncts*. We omit parenthesis in iterated conjuntions and disjunctions. We allow the empty disjunction 0 and the empty conjunction 1, and refer to them as *constants*. Note $\neg 1 = 0$ and $\neg 0 = 1$. A *(k-)term* is a conjunction of (at most k many) literals; and a (k-)*clause* is a disjunction of (at most k many) literals. Both k-terms and k-clauses are said to have *width* k. A *(k-)CNF* is a conjunction of (k-)clauses, and a *(k-)DNF* is a disjunction of (k-)terms.

We define the proof system. A *structural inference* allows to pass from F to G whenever F is a disjunction (or a conjunction) and G has the same set of disjuncts (respectively, conjuncts) as F. Furthermore 0 (respectively, 1) may be freely added or deleted. The system has four further rules of inference, namely *axiom* (AXM) $\frac{}{F \vee \neg F}$ and *weakening* (WKG) $\frac{H}{H \vee F}$, along with *introduction of conjunction* (IOC), and *cut* (CUT):

$$\frac{H \vee F \qquad H' \vee G}{H \vee H' \vee (F \wedge G)} \qquad \frac{H \vee F \qquad H' \vee \neg F}{H \vee H'}.$$

Here, F, G, H and H' are formulas. Note that the common rules $\frac{}{1}$ and $\frac{0}{F}$ (ex falso quodlibet) follow from (AXM) respectively (WKG) plus a structural inference.

A *proof (of G from $F_1, \dots, F_m$)* takes assumptions $F_1, \dots, F_m$ and produces a *conclusion* G through the application of these rules. A *refutation* of $F_1, \dots, F_m$ is a proof of 0 from $F_1, \dots, F_m$. A *(k-)DNF-proof* is one where all formulas are (k-)DNFs. A *resolution proof* is a 1-DNF proof.

By $|F|$ we denote the *size* of the formula F: literals and constants have size 1, and $|(F \wedge G)| = |(F \vee G)| = 1 + |F| + |G|$. Note that $|F| = |\neg F|$. The size of a proof is the sum of the sizes of the formulas it contains.

Lemma 2. *Let s and n be naturals such that $s \geq n \geq 1$ and let $\Gamma \cup \{F\}$ be a set of propositional formulas each of size at most s and mentioning n variables in total. If $\Gamma \models F$, then F has a proof from Γ of size at most $27 \cdot s^2 \cdot 2^n$. Moreover, the proof is a k-DNF proof if each formula in $\Gamma \cup \{F\}$ is a k-DNF.*

We omit the standard proof.

C. Restrictions and decision trees

A *restriction* ρ is a partial assignment, i.e. a function mapping some atoms into $\{0, 1\}$. For a formula F we let $F \restriction \rho$ denote the formula obtained from F by first replacing every atom in the domain of ρ by its value under ρ and then eliminating constants: repeatedly replace subformulas $G \vee 1$ by 1 and $G \wedge 1$ by G; similarly for 0. Note that if the assignment ρ satisfies a literal in clause C, then $C \restriction \rho = 1$. If ρ falsifies a literal in a term T, then $T \restriction \rho = 0$.

A *decision tree* is a finite, rooted, ordered tree whose inner vertices are labeled by atoms, whose leafs are labeled by 0 or 1, and such that no atom occurs twice in a branch (i.e. a path from the root to some leaf). Each inner vertex has two successors (i.e. immediate successors on a branch). Since the tree is ordered we can distinguish between a *left* and a *right* successor of an inner vertex. By a *0-branch* (*1-branch*) we mean a branch leading to a leaf labeled 0 (labeled 1). Every path π from the root to some vertex corresponds to the following restriction that we also denote by π: if an atom occurs as a label of a vertex p in the path π, then the restriction sets this atom to 0 if the left successor of p is in π and to 1 if the right successor of p is in π; if π contains no successor of p, then the restriction does not evaluate the atom.

A decision tree T *represents* a formula F if $F \restriction \pi \equiv b$ for every $b \in \{0,1\}$ and every b-branch π of T. Here, $\equiv$ denotes logical equivalence of formulas. Observe that if T represents F and $F \equiv G$, then T also represents G. The minimal height of a decision tree that represents F is denoted $h(F)$.

Remark 3. The more common definition of representation is stronger than the notion used here in that one demands $F \restriction \pi = b$ for every b-branch π. The choice of the notion of representation is a subtle point; our argument relies on the choice we did, while e.g. some arguments in [12] rely on the stronger notion.

The following lemma is easy to verify.

Lemma 4. *Let F and G be formulas and let T_F and T_G be decision trees of height s_F and s_G that represent F and G, respectively. Then there exists a decision tree T of height at most $s_F + s_G$ that represents $(F \wedge G)$ and such that every 0-branch of T extends some 0-branch of T_F or some 0-branch of T_G.*

Of course, saying that a 0-branch of T extends some 0-branch of T_F means that this holds for the corresponding restrictions.

III. Resilient Expanders

In this section we discuss the sort of expander graphs that we need. In short, these are unbalanced low-degree bipartite expanders that satisfy an additional robustness condition: for at least half the subsets of vertices of some fixed size on the right-hand side, the graph remains an expander if these vertices are removed. Let us note that a similar definition was implicit in [11] which was later revisited in [12]. However, both these concepts were very tied to their specific application to proof complexity. Here we provide a more systematic and general treatment.

A. Definition and some basic properties

Let $G = (U, V, E)$ be a bipartite graph with $|U| = t$ and $|V| = n$ where $t \geq n$. Let b be a positive real and let q and r be naturals such that $0 \leq q \leq n/(1+b)$ and $0 \leq r \leq n$. Recall that G is a (q, b)-expander if $|N_G(S)| \geq (1+b)|S|$ for every q-element subset $S \subseteq U$. We say that G is a (q, b, r)-*resilient expander* if for a random r-element subset $\mathbf{B} \subseteq V$ we have that $G \setminus \mathbf{B}$ is a (q, b)-expander with probability bigger than $1/2$. The choice of $1/2$ here is arbitrary; any constant in the open interval $(0, 1)$ would do. However, observe that if we were to require that $G \setminus \mathbf{B}$ is a (q, b)-expander with probability 1 over the choice of $\mathbf{B}$, then the minimum degree of G would have to exceed r. Later we will see that for the less demanding requirement of probability strictly smaller than 1 we can afford a much smaller degree.

A first property to note is that if G is a (q, b, r)-resilient expander, then $G \cap C$ is also a (q, b, r)-resilient expander for every $C \subseteq U$. In other words, the property is hereditary under taking subsets of the left-hand side. Similarly, if it is a (q, b, r)-resilient expander then it also is a (q', b', r')-resilient expander for all $q' \leq q$, all positive $b' \leq b$, and all $r' \leq r$. The next lemma proves the only non-trivial case of this statement.

Lemma 5. *If G is a (q, b, r)-resilient expander, then G is a (q, b, s)-resilient expander for all $s \leq r$.*

Proof: Fix $s \leq r$. Call a set $B \subseteq V$ good if $G \setminus B$ is a (q, b)-expander. Observe that any subset of a good set is good. Assume at least half the r-element subsets of V are good. Each good r-element set contains exactly $\binom{r}{s}$ many good s-element sets, and each such s-element set appears in at most $\binom{n-s}{r-s}$ many good r-element sets. Therefore, the number of good s-element sets is at least $\frac{1}{2}\binom{n}{r}\binom{r}{s}/\binom{n-s}{r-s}$. Expanding the binomials, one sees this is precisely $\frac{1}{2}\binom{n}{s}$. ∎

B. Existence

We prove that random bipartite graphs with the appropriate parameters are resilient expanders. For naturals t, n and d, let $\mathbf{G} = \mathbf{G}(t, n, d)$ be the random bipartite graph (U, V, E) with $U = [t]$ and $V = [n]$ defined by the following random experiment: for each $u \in U$ choose a d-element subset N_u of V uniformly and independently at random, and declare each $v \in N_u$ a neighbor of u.

Lemma 6. *Let ε and b be positive reals, let t, n, q, r and d be naturals such that $t \geq n > 1 + 2/\varepsilon$, $q \leq n/12(1+b)$, $r \leq n/12$, and $n \geq d \geq (\log t + (3+b)\log n)/(\log n - \log(3(1+b)q + 3r))$, and let $\mathbf{G} = \mathbf{G}(t, n, d)$. Then*

$$\mathbb{P}[\ \mathbf{G} \text{ is a } (q, b, r)\text{-resilient expander }] > 1 - \varepsilon.$$

Before we prove this, let us look at some special cases to illustrate the complicated expressions in the hypothesis. Think of ε and b as positive constants and think of all other parameters as functions of n. If $t = O(n)$, $q = \Omega(n)$ and $r = \Omega(n)$, then the required lower bound on the degree d is $O(\log n)$. On the other hand, if still $t = O(n)$ but $q = n^{1-\Omega(1)}$ and $r = n^{1-\Omega(1)}$, then the required lower bound on the degree is only $O(1)$. For our application we will have $t = 2n$, $q = n^{1-\Omega(1)}$ and $r = \Theta(n/\log n)$, in which case the required lower bound on the degree is $O(\log n/\log\log n)$.

To prove Lemma 6 we rely on the following probabilistic fact. Let X be a random variable that takes all of its values x with positive probability. Given an event $\mathcal{E}$, recall that $\mathbb{P}[\ \mathcal{E} \mid X\ ]$ is the random variable $f \circ X$ where f is the function defined by $f(x) = \mathbb{P}[\ \mathcal{E} \mid X = x\ ]$ for every value x of X.

Lemma 7. *Let p be a real such that $0 < p < 1$, let $\mathcal{E}$ be an event and let X be a random variable. Then*

$$\mathbb{P}[\ \mathbb{P}[\ \mathcal{E} \mid X\ ] > p\ ] \geq \frac{1}{1-p} \cdot (\mathbb{P}[\ \mathcal{E}\ ] - p)\,.$$

Proof: Since $\mathbb{P}[\ \mathcal{E} \mid X\ ]$ takes values in $[0,1]$ we have that $\mathbb{E}[\ \mathbb{P}[\ \mathcal{E} \mid X\ ]\ ]$ is at most

$$\mathbb{P}[\ \mathbb{P}[\ \mathcal{E} \mid X\ ] > p\ ] \cdot 1 + (1 - \mathbb{P}[\ \mathbb{P}[\ \mathcal{E} \mid X\ ] > p\ ]) \cdot p.$$

On the other hand, $\mathbb{E}[\ \mathbb{P}[\ \mathcal{E} \mid X\ ]\ ] = \mathbb{P}[\ \mathcal{E}\ ]$ as can be seen by a direct calculation . This implies the lemma. ■

Proof of Lemma 6: Let $\mathbf{B}$ be an r-element subset of V chosen uniformly at random and independently from $\mathbf{G}$. Let $\mathcal{E}$ be the event that $\mathbf{G} \setminus \mathbf{B}$ is a (q,b)-expander. By Lemma 7 it suffices to show that

$$\mathbb{P}[\ \mathcal{E}\ ] > 1 - \frac{\varepsilon}{2}. \tag{1}$$

Fix B and let $\mathcal{E}^B$ denote the event that $\mathbf{G} \setminus B$ is a (q,b)-expander. Further, fix two sets $S \subseteq U$ and $T \subseteq V \setminus B$ of cardinalities $i \leq q$ and $j < (1+b)i$ respectively. Recall that $N_{\mathbf{G}}(S)$ denotes the neighbors of S in the random graph $\mathbf{G}$. Then

$$\mathbb{P}[\ N_{\mathbf{G}}(S) \subseteq T \cup B\ ] \leq \left(\frac{\binom{j+r}{d}}{\binom{n}{d}}\right)^i \leq \left(\frac{(j+r)e}{n}\right)^{di};$$

here we use $\binom{j+r}{d} \leq ((j+r)e/d)^d$ and $\binom{n}{d} \geq (n/d)^d$. By the union bound over (non-empty) $S \subseteq U$ and $T \subseteq V \setminus B$ of the appropriate cardinalities we have

$$\mathbb{P}[\ \overline{\mathcal{E}^B}\ ] \leq \sum_{i=1}^{q} \binom{t}{i} \sum_{j=1}^{\lfloor (1+b)i \rfloor} \binom{n}{j} \cdot \left(\frac{(j+r)e}{n}\right)^{di}. \tag{2}$$

The term $\binom{n}{j} \cdot ((j+r)e/n)^{di}$ in the internal sum in (2) is bounded by $n^j \cdot ((j+r)e/n)^{di}$, which is an increasing function of j. Plugging in the largest possible j and multiplying by the number of terms, the internal sum in (2) is at most

$$(1+b)i \cdot n^{(1+b)i} \cdot \left(\frac{(1+b)ie + re}{n}\right)^{di} \leq \left(n^{2+b} \cdot \left(\frac{3(1+b)q + 3r}{n}\right)^d\right)^i.$$

Here we use $1 \leq i \leq q$ and $q \leq n/12(1+b)$ so that $(1+b)i \leq n$ and $(1+b)i \cdot n^{(1+b)i} \leq n^{(2+b)i}$. Crudely bounding $\binom{t}{i}$ by t^i, we conclude that (2) is bounded by

$$\sum_{i=1}^{q} \left(t \cdot n^{2+b} \cdot \left(\frac{3(1+b)q + 3r}{n}\right)^d\right)^i.$$

From $q \leq n/12(1+b)$ and $r \leq n/12$ we conclude that the fraction is bounded by $1/2$ and hence is strictly smaller than 1. From $d \geq (\log t + (3+b)\log n)/(\log n - \log(3(1+b)q + 3r))$ we conclude that (2) is bounded by

$$\sum_{i=1}^{\infty} \left(\frac{1}{n}\right)^i = \frac{1}{n-1}.$$

At this point we proved that $\mathbb{P}[\ \overline{\mathcal{E}^B}\ ] \leq 1/(n-1)$ for every B. This implies (1), because

$$\begin{aligned} \mathbb{P}[\ \overline{\mathcal{E}}\ ] &= \sum_B \mathbb{P}[\ \overline{\mathcal{E}^B} \text{ and } \mathbf{B} = B\ ] \\ &= \sum_B \mathbb{P}[\ \overline{\mathcal{E}^B}\ ] \cdot \mathbb{P}[\ \mathbf{B} = B\ ] \\ &\leq \frac{1}{n-1} < \frac{\varepsilon}{2}. \end{aligned}$$

Here, the second displayed equality is due to the independence of the events $\overline{\mathcal{E}^B}$ and $\mathbf{B} = B$, and the last inequality is due to $n > 1 + 2/\varepsilon$. ■

C. Left and right degrees

Besides being a resilient-expander, we often need our graph to have low right-degree. This is guaranteed in a random graph by the following easy calculation:

Lemma 8. *Let ε be a positive real, let t, n, d and d' be naturals satisfying $t \geq n \geq d$ and $n(tde/nd')^{d'} < \varepsilon$, and let $\mathbf{G} = \mathbf{G}(t,n,d)$. Then*

$$\mathbb{P}[\ \mathbf{G} \textit{ has right-degree smaller than } d'\ ] > 1 - \varepsilon.$$

Proof: For fixed vertices $u \in U$ and $v \in V$, the probability that (u,v) is an edge in $\mathbf{G}$ is $\binom{n-1}{d-1}/\binom{n}{d} = d/n$. Moreover, for fixed $v \in V$, these events are mutually independent as u ranges over U. By the union

bound over all d'-element subsets of U, this means that the probability that the degree of v is at least d' is bounded by $\binom{t}{d'}(d/n)^{d'}$. By the union bound over v, the probability that the right-degree is at least d' is bounded by $n\binom{t}{d'}(d/n)^{d'}$. The lemma follows from the bound $\binom{t}{d'} \leq (te/d')^{d'}$ and the hypothesis that $n(tde/nd')^{d'} < \varepsilon$. ∎

As mentioned earlier, in our application of Lemma 6 we will have $b = O(1)$, $t = 2n$, $q = n^{1-\Omega(1)}$ and $r = \Theta(n/\log n)$, in which case the required lower bound on d is $O(\log n/\log\log n)$. Setting $d = \lceil \log n \rceil$ satisfies this lower bound and Lemma 8 gives right-degree $d' = O(\log n)$. Therefore, for the setting of parameters b, t, q and r of our interest, there exists a (q, b, r)-resilient expander with left-degree $O(\log n)$ and right-degree $O(\log n)$. Let us argue now that having a (q, b, r)-resilient expander with right-degree $O(\log n)$ but left-degree $o(\log n/\log\log n)$ is impossible.

Suppose G is an (t, n, d_L, d_R)-graph that is a (q, b, r)-resilient expander where b, t, q and r are as above and $d_R = O(\log n)$. Then there exist at least $t/(d_L \cdot d_R)$ vertices in U with pairwise disjoint neighborhoods in V. Let $\tilde{\mathbf{B}}$ be a random subset of V obtained by placing each vertex in it independently with probability r/n. For a fixed vertex $u \in U$, the probability that $\tilde{\mathbf{B}}$ contains all the neighbors of u is at least $(r/n)^{d_L}$. Moreover, these events are mutually independent for vertices from U that have pairwise disjoint neighborhoods in V. Therefore, the probability that $\tilde{\mathbf{B}}$ does not contain all the neighbors of any vertex in U is bounded by

$$\left(1 - \left(\frac{r}{n}\right)^{d_L}\right)^{\frac{t}{d_L \cdot d_R}} \leq \exp\left(-\left(\frac{r}{n}\right)^{d_L} \cdot \frac{t}{d_L \cdot d_R}\right).$$

The probability of this event for a random r-element subset $\mathbf{B} \subseteq V$ is at most a multiplicative factor $3\sqrt{r}$ bigger (see equation (5) in Section IV). Since G is a (q, b, r)-resilient expander, the probability of this event for $\mathbf{B}$ is at least $1/2$. But since $t \geq n$, $r = \Omega(n/\log n)$ and $d_R = O(\log n)$, this is possible only if d_L is $\Omega(\log n/\log\log n)$.

IV. Proof

In this section we develop the proof of Theorem 1 as outlined in the introduction.

A. Killing large conjunctions

Let t be a natural such that $n < t < m$. Let $\boldsymbol{\rho} = \boldsymbol{\rho}(t)$ be the random restriction on the variables of $PHP_n^{m,t}$ defined by the following random experiment (of course, by a random restriction we mean a random variable whose values are restrictions):

1) choose a subset $\mathbf{A} \subseteq [m]$ uniformly at random among all t-element subsets of $[m]$.
2) let $\boldsymbol{\rho}$ be the restriction that, for every $u \in [m]$, sets R_u to 1 if $u \in \mathbf{A}$ and to 0 otherwise;
3) extend $\boldsymbol{\rho}$ to set the auxiliary variables $\bar{X}$ such that $\mathrm{TH}_t(\bar{R}, \bar{X})$ is satisfied;
4) extend $\boldsymbol{\rho}$ to set every $P_{u,v}$ with $u \in [m] \setminus \mathbf{A}$ and $v \in [n]$ to 1 independently with probability $1/2$ and to 0 otherwise.

Here, by a *pigeon variable* we mean a variable $P_{u,v}$ for $u \in [m]$ and $v \in [n]$; we say $P_{u,v}$ *mentions* pigeon u; a formula *mentions* a pigeon if so does some variable occuring in it.

For later use, note that if ρ is a realization of $\boldsymbol{\rho}$ and A is the corresponding realization of $\mathbf{A}$, then $PHP_n^{m,t} \restriction \rho$ and PHP_n^t are the same formula up to renaming of pigeons.

Lemma 9. *Let p be a natural such that $p < t$ and $p < m - t$, and T be a term that mentions at least p many pigeons. Then*

$$\mathbb{P}[\, T \restriction \boldsymbol{\rho} \neq 0 \,] \leq \left(\frac{1}{2} + \frac{t}{m-p}\right)^p.$$

Proof: Choose p literals in T mentioning pairwise different pigeons. Let P be the set of pigeons mentioned by these literals, and for every $u \in P$ let ℓ_u be the literal chosen for pigeon u. Consider the events $\mathcal{E} :=$ "$\boldsymbol{\rho}(\ell_u) \neq 0$ for all $u \in P \setminus \mathbf{A}$", and $\mathcal{F}_i :=$ "$|P \setminus \mathbf{A}| = i$", where $i \in \{0, \ldots, p\}$. Note that $\mathbb{P}[\, T \restriction \boldsymbol{\rho} \neq 0 \,] \leq \mathbb{P}[\, \mathcal{E} \,]$ and

$$\begin{aligned}\mathbb{P}[\, \mathcal{E} \,] &= \sum_{i=0}^{p} \mathbb{P}[\, \mathcal{E} \mid \mathcal{F}_i \,] \cdot \mathbb{P}[\, \mathcal{F}_i \,] \\ &= \sum_{i=0}^{p} \frac{1}{2^i} \cdot \frac{\binom{p}{i}\binom{m-p}{t-p+i}}{\binom{m}{t}}.\end{aligned}$$

For naturals $m \geq k$ we write $m^{\underline{k}}$ for the falling factorial $m^{\underline{k}} := m \cdot (m-1) \cdots (m-k+1)$. Note that our assumptions on p ensure $m - p > t - p + i > 0$. Using $0 \leq i \leq p$ and noting $m^{\underline{p}} = m^{\underline{i}} \cdot (m-i)^{\underline{p-i}}$, we have

$$\frac{\binom{m-p}{t-p+i}}{\binom{m}{t}} = \frac{(m-t)^{\underline{i}}}{m^{\underline{i}}} \cdot \frac{t^{\underline{p-i}}}{(m-i)^{\underline{p-i}}} \leq \frac{t^{\underline{p-i}}}{(m-i)^{\underline{p-i}}}$$

and this is at most $\left(\frac{t}{m-p}\right)^{p-i}$. Replacing, and using the binomial formula, the probability we want is at most

$$\sum_{i=0}^{p} \binom{p}{i} \cdot \left(\frac{1}{2}\right)^i \cdot \left(\frac{t}{m-p}\right)^{p-i} = \left(\frac{1}{2} + \frac{t}{m-p}\right)^p,$$

as claimed. ∎

Lemma 10. *Let p and s be naturals such that $s < p < t$, and T be a term that mentions at most p many pigeons.*

Then the probability of the event that $T \restriction \boldsymbol{\rho}$ mentions more than s many pigeons, is at most

$$\binom{p}{s+1}\left(\frac{t}{m}\right)^{s+1}.$$

Proof: For any $s+1$ pigeon variables in T mentioning pairwise different pigeons, the probability that they all remain unset by $\boldsymbol{\rho}$ is

$$\frac{\binom{m-s-1}{t-s-1}}{\binom{m}{t}} = \frac{t^{\underline{s+1}}}{m^{\underline{s+1}}} \leq \left(\frac{t}{m}\right)^{s+1}.$$

The claim thus follows by the union bound. ∎

B. Restriction to a graph and binary encoding

Let t be a natural such that $n < t < m$ and let $G = (U, V, E)$ be a bipartite graph with $U = [t]$ and $V = [n]$. Consider the following restriction θ_G: it sets every variable $P_{u,v}$ to 0 if $(u,v) \notin E$ and is undefined on all other variables. Then $\mathit{PHP}^t_n \restriction \theta_G$ is the CNF with clauses (1 and)

$$\begin{array}{ll} \bigvee_{v \in N_G(u)} P_{u,v} & \text{for } u \in U, \\ \neg P_{u,v} \vee \neg P_{u',v} & \text{for } (u,v),(u',v) \in E \text{ with } u \neq u'. \end{array}$$

This CNF is denoted $\mathit{PHP}(G)$ (cf. [20]).

Now assume that G is a (U, V, d_L, d_R)-graph with associated function ϕ_G. Write $\ell := |d_L - 1|$ for the length of the binary representation of the largest number in $[d_L]$. We introduce *binary pigeon variables* $P_{u;b}$ for $u \in U$ and $b \in [\ell]$. Again, we say that $P_{u;b}$ *mentions* pigeon u, and that a formula mentions the pigeons mentioned by some atom occuring in it. The intuitive meaning of a truth assignment to the binary pigeon variables is that pigeon u flies to hole $\phi_G(u,j)$, where j is the number whose binary representation is given by the truth values $P_{u;\ell-1}, \ldots, P_{u;0}$. The formula $\mathit{BPHP}(G)$ has *domain clauses*

$$\bigvee_{b \in [\ell]} \neg^{\mathrm{bit}(b,j)} P_{u;b}$$

for $(u,j) \in U \times [2^\ell]$ such that $(u,j) \notin \mathrm{Dom}(\phi_G)$, and *collision clauses*:

$$\bigvee_{b \in [\ell]} \neg^{\mathrm{bit}(b,j)} P_{u;b} \vee \bigvee_{b \in [\ell]} \neg^{\mathrm{bit}(b,j')} P_{u';b}$$

for $(u,j) \in \mathrm{Dom}(\phi_G)$ and $(u',j') \in \mathrm{Dom}(\phi_G)$ such that $u \neq u'$ and $\phi_G(u,j) = \phi_G(u',j')$. Here, for a variable X we write $\neg^0 X := X$ and $\neg^1 X := \neg X$.

The unary encoding $\mathit{PHP}(G)$ and the binary encoding $\mathit{BPHP}(G)$ are closely related. Indeed, the formula obtained from $\mathit{PHP}(G)$ by substituting every variable $P_{u,v}$ by the term $\bigwedge_{b \in [\ell]} \neg^{1-\mathrm{bit}(b,j)} P_{u;b}$, where $j \in [2^\ell]$ is such that $\phi(u,j) = v$, is the conjunction of the collision clauses of $\mathit{BPHP}(G)$ and *sporadic axioms*:

$$\bigvee_{j \in J_G(u)} \bigwedge_{b \in [\ell]} \neg^{1-\mathrm{bit}(b,j)} P_{u;b}$$

for $u \in U$ where $J_G(u)$ denotes the set $\{j \in [2^\ell] \mid (u,j) \in \mathrm{Dom}(\phi_G)\}$. The following lemma states that these sporadic axioms are redundant.

Lemma 11. *Every sporadic axiom has a DNF-proof from the domain clauses of $\mathit{BPHP}(G)$ of size at most $112 \cdot \ell^2 \cdot 8^\ell$ and such that every term appearing in the proof mentions one pigeon.*

Proof: Observe that for $u \in U$ the formula

$$\bigvee_{j \in [2^\ell]} \bigwedge_{b \in [\ell]} \neg^{1-\mathrm{bit}(b,j)} P_{u;b}$$

is a tautology in the ℓ variables that mention pigeon u and has size $2^\ell \cdot (\ell + (\ell - 1)) + (2^\ell - 1) \leq \ell \cdot 2^{\ell+1}$. By Lemma 2 it has a DNF-proof of size at most $27 \cdot \ell^2 \cdot 2^{3\ell+2}$. The sporadic axiom is obtained from this tautology, written appropriately via one structural inference, by at most 2^ℓ many cuts with domain clauses of size at most 2ℓ each. This adds a factor of at most $(1 + 2^\ell) \cdot \ell \cdot 2^{\ell+1} \cdot 2\ell \leq \ell^2 \cdot 2^{2\ell+3}$ in size. In total, the proof has size at most $28 \cdot \ell^2 \cdot 2^{3\ell+2}$. ∎

C. Killing large disjunctions

Let t be a natural such that $n < t < m$ and let $G = (U, V, E)$ be a (t, n, d_L, d_R)-graph with associated function ϕ_G. Let r be a natural such that $1 \leq r \leq n$. We define a random restriction $\boldsymbol{\mu} = \boldsymbol{\mu}(G, r)$ on the variables of $\mathit{BPHP}(G)$ by the following random experiment:

1) independently for every $v \in V$, choose a pigeon $\mathbf{Q}_v \in N_G(v)$ uniformly at random;
2) independently, choose a subset $\mathbf{B} \subseteq V$ uniformly at random among all r-element subsets of V;
3) let $\mathbf{M} := \{(\mathbf{Q}_v, v) \mid v \in \mathbf{B} \text{ and } \mathbf{Q}_v \neq \mathbf{Q}_{v'} \text{ for all } v' \in \mathbf{B} \setminus \{v\}\}$;
4) let $\boldsymbol{\mu}$ be the partial assignment associated with the matching $\mathbf{M}$.

Here, the partial assignment μ associated with a matching M of G is the assignment that, for every $(u,v) \in M$, sets $P_{u;b}$ to $\mathrm{bit}(b,j)$ for every $b \in [\ell]$, where j is such that $\phi_G(u,j) = v$, and leaves the other variables unset. Call a formula F *matching-satisfiable (in G)* if $F \restriction \mu = 1$ for some such partial assignment μ. Two formulas F and F' are *very disjoint (in G)* if $N_G(P)$ and $N_G(P')$ are disjoint, where $P \subseteq U$ and $P' \subseteq U$ are the sets of pigeons mentioned by F and F' respectively.

Lemma 12. *Let s and w be naturals such that $r \geq s \geq 1$ and $w \geq 1$. Further, let $F = \bigvee \Gamma$ where Γ contains at least w matching-satisfiable, pairwise very disjoint formulas each mentioning at most s pigeons. Then the probability of the event that $F \restriction \boldsymbol{\mu} \neq 1$ is at most*

$$3\sqrt{r} \cdot \exp\left(-w \cdot \left(\frac{r}{d_R \cdot n}\right)^s \cdot \left(1 - \frac{r}{n}\right)^{d_L \cdot s}\right).$$

Proof: Define the random variables $\tilde{\mathbf{B}}$, $(\tilde{\mathbf{Q}}_v)_{v\in V}$, $\tilde{\mathbf{M}}$, $\tilde{\boldsymbol{\mu}}$ similarly as above but letting $\tilde{\mathbf{B}}$ be the random subset of V that contains every $v \in V$ independently with probability r/n. Let $\tilde{\mathbf{B}}_v$ denote the indicator variable for the event that $v \in \tilde{\mathbf{B}}$; note that the indicator variables are independent.

Fix a matching-satisfiable formula $F' \in \Gamma$ mentioning at most s pigeons. Choose a minimal matching M such that $F' \restriction \mu = 1$ where μ is the partial assignment associated with M. Write $M_0 := \mathrm{Dom}(M)$ and $M_1 := \mathrm{Im}(M)$. Then, by minimality of M, the domain M_0 is included in the set of pigeons $P \subseteq U$ mentioned by F'. Observe that the event that $F' \restriction \tilde{\boldsymbol{\mu}} = 1$ is implied by the event that $M \subseteq \tilde{\mathbf{M}}$. The latter event is implied by the intersection of

$$\mathcal{E}_1 := \text{“}\tilde{\mathbf{B}}_v = 1 \text{ for every } v \in M_1\text{”, and}$$
$$\mathcal{E}_2 := \text{“}\tilde{\mathbf{Q}}_v = M^{-1}(v) \text{ for every } v \in M_1\text{”}$$

and the event that $\tilde{\mathbf{Q}}_v \notin M_0$ for every $v \in \tilde{\mathbf{B}} \setminus M_1$. Thus it is implied by the intersection of $\mathcal{E}_1$, $\mathcal{E}_2$ and

$$\mathcal{E}_3 := \text{“}\tilde{\mathbf{B}}_v = 0 \text{ for every } v \in N_G(M_0) \setminus M_1\text{”}.$$

Now, the probability of $\mathcal{E}_1$ is at least $(r/n)^s$, the probability of $\mathcal{E}_2$ is at least $(1/d_R)^s$, and the probability of $\mathcal{E}_3$ is at least $(1-r/n)^{d_L\cdot s}$, the last because $|N_G(M_0)\setminus M_1| \leq d_L \cdot s$. These three events are independent. Hence

$$\mathbb{P}[\ \mathcal{E}_1 \cap \mathcal{E}_2 \cap \mathcal{E}_3\ ] \geq \left(\frac{r}{n}\right)^s \cdot \left(\frac{1}{d_R}\right)^s \cdot \left(1-\frac{r}{n}\right)^{d_L\cdot s} =: p.$$

The event $\mathcal{E}_1 \cap \mathcal{E}_2 \cap \mathcal{E}_3$ depends only on the variables $\tilde{\mathbf{Q}}_v$ and $\tilde{\mathbf{B}}_v$ with $v \in N_G(M_0) \subseteq N_G(P)$. Thus, for a family of pairwise very disjoint formulas in Γ, the events are independent. Using the assumption of the lemma,

$$\mathbb{P}[\ F \restriction \tilde{\boldsymbol{\mu}} \neq 1\ ] \leq (1-p)^w \leq \exp(-wp). \tag{3}$$

Writing $B(m,q)(k) = \binom{m}{k} q^k (1-q)^{m-k}$ for the binomial distribution, we have

$$\begin{aligned}\mathbb{P}[F \restriction \tilde{\boldsymbol{\mu}} \neq 1] &\geq \mathbb{P}[|\tilde{\mathbf{B}}| = r] \cdot \mathbb{P}[F \restriction \tilde{\boldsymbol{\mu}} \neq 1 \mid |\tilde{\mathbf{B}}| = r] \\ &= B\left(n, \frac{r}{n}\right)(r) \cdot \mathbb{P}[F \restriction \boldsymbol{\mu}]. \end{aligned} \tag{4}$$

Using Robbins' [22] version of Stirling's formula, one can derive the following bound (see also [23, p.4, Eq. (1.5)]):

$$B\left(n, \frac{r}{n}\right)(r) \geq \frac{1}{e^{1/6}} \cdot \frac{1}{\sqrt{2\pi}} \cdot \left(\frac{n}{r(n-r)}\right)^{1/2} \geq \frac{1}{3}\frac{1}{\sqrt{r}}. \tag{5}$$

Combining (3), (4) and (5) yields the lemma. ∎

Again, we write $\ell := |d_L - 1|$.

Lemma 13. *Let s, s_0 and s_1 be naturals such that $s \geq 1$ and $s_0 \geq s_1 \geq 2\ell$. If BPHP(G) has a refutation of size at most s_0 such that every formula in it has the form $\bigvee\Gamma$ for some set Γ of ℓ-CNFs each of which has size at most s_1 and mentions at most s pigeons (we allow a singleton Γ and understand that $\bigvee\{F\} = F$), then BPHP(G) has a refutation of size at most $s_0 \cdot 729 \cdot s_1^4 \cdot 4^{s\cdot\ell}$ such that every formula in it has the form $\bigvee\Gamma$ for some set Γ of ℓ-CNFs each of which mentions at most s pigeons and is matching-satisfiable.*

Proof: Consider an (IOC)-application that introduces a ℓ-CNF F which is not matching-satisfiable. Let Δ be the set of clauses from *BPHP*(G) that mention exactly the at most s many pigeons mentioned by F. Then $\Delta \models \neg F$ because any assignment to the pigeon variables appearing in Δ satisfies every clause in Δ only if it is associated to some matching. Since there are at most $s \cdot \ell$ variables mentioning the s many pigeons in F, by Lemma 2 there is a proof of $\neg F$ from Δ of size at most $27 \cdot s_1^2 \cdot 2^{s\cdot\ell}$. Add this proof to the refutation; a structural inference on $\neg F$ and two cuts with the premisses of the (IOC) application derives the formula without F; this formula can be used to continue the proof. Proceed like this for all (IOC)-applications in the original proof. For each F eliminated in this way we added a proof of the ℓ-DNF $\neg F$ and this proof may contain new formulas which are not matching-satisfiable. But this proof can be chosen as an ℓ-DNF-proof where each ℓ-term mentions at most s many pigeons. As above, eliminate all the new ℓ-terms T which are not matching-satisfiable. The required proofs of the clause $\neg T$ can now be chosen as resolution proofs of size at most $27 \cdot (\ell + (\ell-1))^2 \cdot 2^\ell$. In these resolution proofs all formulas are disjunctions of literals and every literal is matching-satisfiable – at least if every pigeon u has at least one neighbor in G. This we can assume because otherwise already the domain clauses for u are contradictory and have a resolution refutation of size at most $27 \cdot (\ell + (\ell-1))^2 \cdot 2^\ell$. ∎

D. Switching lemma

Associate with a DNF F the hypergraph $\mathcal{H}(F)$ which has as universe the set of variables of F and which has for each term T in F a hyperedge consisting in the variables of T. The *covering number* $\mathrm{cv}(F)$ of F is the size of the smallest hitting set of $\mathcal{H}(F)$.

Lemma 14. *Let F be a k-DNF in the binary pigeon variables. Then F contains at least*

$$\frac{\mathrm{cv}(F)}{\ell \cdot k \cdot d_L \cdot d_R}$$

many pairwise very disjoint terms.

Proof: Let $\mathcal{T}$ be a maximal family of very disjoint terms in F. Let P be the set of pigeons mentioned by $\bigvee\mathcal{T}$. Then the set of all pigeon variables mentioning

pigeons in $N_G(N_G(P))$ is a hitting set of $\mathcal{H}(F)$. Noting that $N_G(N_G(P))$ has cardinality at most $|\mathcal{T}| \cdot d_L \cdot d_R$ we get

$$\mathrm{cv}(F) \leq |N_G(N_G(P))| \leq |\mathcal{T}| \cdot \ell \cdot k \cdot d_L \cdot d_R$$

and the lemma follows. ∎

Interest in the covering number stems from the following lemma proved in by Segerlind, Buss and Impagliazzo [12] (see also the survey [21, Corollary 9.3]).

Lemma 15 ([12])**.** *Let $k, h, c > 0$ be naturals and $\gamma > 0$ a real. Let Γ be a set of k-DNFs that is closed under restrictions and assume that $\boldsymbol{\sigma}$ is a random restriction such that $\mathbb{P}[\, F \restriction \boldsymbol{\sigma} \neq 1 \,] \leq c \cdot 2^{-\gamma \cdot \mathrm{cv}(F)}$ for every $F \in \Gamma$. Then for every $F \in \Gamma$ we have*

$$\mathbb{P}\big[\, h(F \restriction \boldsymbol{\sigma}) > h \,\big] \leq c \cdot k \cdot 2^{-(\gamma/4)^k \cdot h}.$$

Recall, $h(F)$ denotes the minimal height of a decision tree representing the formula F.

E. Matching game

In the next section we show that if G is a good expander, then all the refutations of *BPHP*(G) involve some formula that cannot be represented by a shallow decision tree. For its proof we use the *matching games* from [24] later simplified in [25]. Here we provide even cleaner proofs.

Let G be a (U, V, d_L, d_R)-graph. For $S \subseteq U$ and $T \subseteq V$, we say that S *is matchable into* T if there exists a matching M of G with $S \subseteq \mathrm{Dom}(M)$ and $\mathrm{Im}(M) \subseteq T$. If S is not matchable into T but every proper subset of S is, we call it *minimally non-matchable*. For a matching M and a natural $q > 0$, we say that M is *q-extendible* if every $S \subseteq U \setminus \mathrm{Dom}(M)$ of cardinality at most q is matchable into $V \setminus \mathrm{Im}(M)$.

Lemma 16. *Let $q > 0$ be a natural. If M is a q-extendible matching and (u, v) is an edge in M, then $M \setminus \{(u, v)\}$ is a q-extendible matching.*

Proof: Write $M_0 := \mathrm{Dom}(M)$ and $M_1 := \mathrm{Im}(M)$ and note that $u \in M_0$ and $v \in M_1$. Let S' be a subset of $U \setminus (M_0 \setminus \{u\})$ of cardinality at most q. We need to show that S' is matchable into $V \setminus (M_1 \setminus \{v\})$. We consider two cases: $u \in S'$ and $u \notin S'$. In case $u \in S'$, using that $u \in M_0$, we have that $S' \setminus \{u\}$ is a subset of $U \setminus M_0$ of cardinality at most q. Since M is q-extendible, $S' \setminus \{u\}$ is matchable into $V \setminus M_1$. But then, using that $v \in M_1$, the set S' is also matchable into $V \setminus (M_1 \setminus \{v\})$ by adding (u, v) to the matching that witnesses this. In case $u \notin S'$ then S' is a subset of $U \setminus M_0$ of cardinality at most q. Since M is q-extendible we conclude that S' is matchable into $V \setminus M_1$, and hence into $V \setminus (M_1 \setminus \{v\})$. ∎

For a natural $q > 0$ and a real $b > 0$, the graph G is a (q, b)-*expander* if $|N_G(S)| \geq (1 + b)|S|$ for every $S \subseteq U$ of cardinality at most q.

Lemma 17. *Let $q > 0$ be a natural and $b > 0$ a real. If G is a (q, b)-expander, M is a q-extendible matching with $|M| < \lfloor qb/d_L \rfloor$ and $u \in U \setminus \mathrm{Dom}(M)$, then there exists $v \in N_G(u) \setminus \mathrm{Im}(M)$ such that $M \cup \{(u, v)\}$ is a q-extendible matching.*

Proof: Again write $M_0 := \mathrm{Dom}(M)$ and $M_1 := \mathrm{Im}(M)$. Let $v_1, \ldots, v_l$ be an enumeration of $N_G(u) \setminus M_1$. Since M is q-extendible and $q \geq 1$, we have that $\{u\}$ is matchable into $V \setminus M_1$, so $l \geq 1$. Clearly, $M \cup \{(u, v_i)\}$ is a matching for every $i \in \{1, \ldots, l\}$. Assume for contradiction that $M \cup \{(u, v_i)\}$ is not q-extendible for any $i \in \{1, \ldots, l\}$. For every $i \in \{1, \ldots, l\}$ let S_i be a subset of $U \setminus (M_0 \cup \{u\})$ of cardinality at most q that is minimally non-matchable into $V \setminus (M_1 \cup \{v_i\})$. By Hall's Theorem and the minimality of S_i we have $|N_G(S_i) \setminus (M_1 \cup \{v_i\})| < |S_i|$, and hence $|N_G(S_i)| < |S_i| + (qb/d_L - 1) + 1$. On the other hand $|S_i| \leq q$, and hence $|N_G(S_i)| \geq (1 + b)|S_i|$ by expansion of G. These together imply $|S_i| < q/d_L$ and hence $|S_i| < q/l$ because $1 \leq l \leq d_L$. Since this holds for every $i \in \{1, \ldots, l\}$ we get $|S| \leq q$ for $S := \bigcup_{i=1}^{l} S_i \cup \{u\}$. Since M is q-extendible and $S \subseteq U \setminus M_0$ we conclude that S is matchable into $V \setminus M_1$. A matching M' witnessing this matches u to v_i for some $i \in \{1, \ldots, l\}$. As M' matches S_i into $V \setminus M_1$ while S_i is non-matchable into $V \setminus (M_1 \cup \{v_i\})$, necessarily M' matches some $u_i \in S_i$ to v_i. But this contradicts M' being matching because $u_i \neq u$ as $u \notin S_i$. ∎

F. Adversary argument

Let G be a (U, V, d_L, d_R)-graph. We derive a lower bound on the height of formulas in a refutation of *BPHP*(G) provided G is suitably expanding. This is done by an adversary argument (cf. [26]) based on Lemma 17.

Lemma 18. *Let $q > 0$ be a natural and $b > 0$ a real. If G is a (q, b)-expander, then every refutation of BPHP(G) contains a formula F with*

$$h(F) > \tfrac{1}{3}\lfloor qb/d_L \rfloor.$$

Proof: For the sake of contradiction assume $F_0, \ldots, F_{s-1}$ is a refutation of *BPHP*(G) such that $h(F_i) \leq \frac{1}{3}\lfloor qb/d_L \rfloor$ for all $i \in [s]$; let T_i be a decision tree of height $\leq \frac{1}{3}\lfloor qb/d_L \rfloor$ representing F_i and assume T_{s-1} is the tree with one node labeled 0. We can

assume that every F_i contains only variables occurring in *BPHP*(G): otherwise substitute 0 for all other variables and "answer" in T_i all queries on these variables by 0.

For a matching M let μ_M denote the restriction associated with it (cf. Section IV-C).

Claim. Let M be a matching and $i \in [s]$. Then

1) if F_i is a clause in *BPHP*(G) or an axiom, then $F_i \restriction \mu_M \not\equiv 0$,
2) if M is q-extendible and such that $|M| \leq \frac{1}{3}\lfloor qb/d_L \rfloor$ and $F_i \restriction \mu_M \equiv 0$, then there exists $1 \leq i' < i$ and a q-extendible matching M' such that $|M'| \leq \frac{1}{3}\lfloor qb/d_L \rfloor$ and $F_{i'} \restriction \mu_{M'} \equiv 0$.

Proof of Claim. The first item is trivial if F_i is an axiom. Assume F_i is a domain clause for $(u, j) \notin \mathrm{Dom}(\phi_G)$. If $u \notin \mathrm{Dom}(M)$, then F_i is untouched by μ_M. Otherwise there is j' such that $\phi(u, j') = M(u)$. Then $j \neq j'$ and there is a $b \in [\ell]$ such that $\mathrm{bit}(b, j) \neq \mathrm{bit}(b, j')$. Then μ_M evaluates $P_{u;b}$ to $\mathrm{bit}(b, j')$, and hence $\neg^{\mathrm{bit}(b,j)} P_{u;b} \restriction \mu_M = 1$. Then $F_i \restriction \mu_M = 1$, so $F_i \restriction \mu_M \not\equiv 0$.

Assume F_i is a collision clause for u, u', j, j' with $u \neq u'$ and $\phi_G(u, j) = \phi_G(u, j')$. If not both u and u' are in $\mathrm{Dom}(M)$, then clearly $F_i \restriction \mu_M \not\equiv 0$. Otherwise, as M is a matching, $M(u) \neq \phi_G(u, j)$ or $M(u') \neq \phi_G(u', j')$. Assume the first and choose j'' such that $M(u) = \phi_G(u, j'')$. Then $j \neq j''$, so $\mathrm{bit}(b, j) \neq \mathrm{bit}(b, j'')$ for some $b \in [\ell]$. As above, this implies $\neg^{\mathrm{bit}(b,j)} P_{u;b} \restriction \mu_M = 1$, so $F_i \restriction \mu_M = 1$ and $F_i \restriction \mu_M \not\equiv 0$.

We now prove the second item. Let i and M accord its assumption. By the first item, F_i is not a clause in *BPHP*(G) nor an axiom. Then there are $i_0, i_1 < i$ such that F_i is logically implied by $(F_{i_0} \wedge F_{i_1})$. By Lemma 4 there is a decision tree T of height $\leq \frac{2}{3}\lfloor qb/d_L \rfloor$ that represents $(F_{i_0} \wedge F_{i_1})$.

We call a matching *appropriate for* a path π in T if it is q-extendible, contains M, its associated restriction extends π (as a restriction, cf. Section II-C), and its domain is $\mathrm{Dom}(M) \cup U(\pi)$, where $U(\pi)$ is the set of pigeons mentioned by some variable queried in π.

Subclaim. There exists a branch π of T and a matching M_π appropriate for π.

The subclaim implies the Claim: if π were a 1-branch, then $(F_{i_0} \wedge F_{i_1}) \restriction \mu_{M_\pi} \equiv 1$ (since μ_{M_π} extends π), so $F_i \restriction \mu_{M_\pi} \equiv 1$ and this contradicts $M \subseteq M_\pi$ and $F_i \restriction \mu_M \equiv 0$. Hence π is a 0-branch and thus extends a 0-branch π' of T_{i_0} or T_{i_1}. Choose accordingly $i' := i_0$ or $i' := i_1$ and let M' be the restriction of M_π to $U(\pi')$. Then M' is q-extendible (by Lemma 16), $|M'| \leq \frac{1}{3}\lfloor qb/d_L \rfloor$ (since $|U(\pi')| \leq \frac{1}{3}\lfloor qb/d \rfloor$) and $F_{i'} \restriction \mu_{M'} \equiv 0$ (since $\mu_{M'}$ extends π').

Observe that M is an appropriate matching for the path π consisting only in the root of T. To prove the subclaim it thus suffices to show that if we have a path π with appropriate matching M_π such that π that does not lead to a leaf of T then we can extend π by one node t such that there is an appropriate matching $M_{\pi t}$ for πt.

So let π and M_π be as stated, say, π leads to an inner node t of T querying the variable $P_{u;b}$. We distinguish two cases. In case $u \in \mathrm{Dom}(M_\pi)$ then μ_{M_π} evaluates $P_{u;b}$; in this case we prolongue π by the corresponding successor t' of t and let $M_{\pi t'} := M_\pi$. In case $u \notin \mathrm{Dom}(M_\pi)$ we look for some v such that $M_\pi \cup \{(u, v)\}$ is a q-extendible matching and then proceed as in the first case. Such a v can be found because $\mathrm{Dom}(M_\pi) = \mathrm{Dom}(M) \cup U(\pi)$ has cardinality at most

$$|\mathrm{Dom}(M)| + |U(\pi)| \quad \leq \quad \tfrac{1}{3}\lfloor qb/d_L \rfloor + \tfrac{2}{3}\lfloor qb/d_L \rfloor - 1$$

and thus smaller than $\lfloor qb/d_L \rfloor$, so Lemma 17 applies. Here we use that $|U(\pi)|$ is bounded by the length of π, and this is at most $\frac{2}{3}\lfloor qb/d_L \rfloor - 1$ because π leads to an internal node of T, whose height is $\leq \frac{2}{3}\lfloor qb/d_L \rfloor$. ⊣

The Claim implies that there are no i and M that satisfy the assumption of the second item. But $i := s - 1$ and $M := \emptyset$ do: using Hall's Theorem it is easy to see that $\emptyset$ is q-extendible, and obviously $0 \leq \frac{1}{3}\lfloor qb/d_L \rfloor$ and $F_{s-1} \restriction \emptyset \equiv 0$ hold because $F_{s-1} = 0$. ■

G. Proof size lower bound

We prove Theorem 1. Let $\epsilon > 0$ be arbitrary and write

$$m := n^2,\ t := 2n,\ s := (\log n)^{1/2-\epsilon}.$$

Assume for the sake of contradiction that there exists infinitely many n such that $PHP_n^{m,t}$ has a DNF-refutation $R = R_n$ of size at most n^s. For the next claim recall the random restriction $\boldsymbol{\rho} = \boldsymbol{\rho}(t)$ from Section IV-A.

Claim 1. There exists a realization ρ of $\boldsymbol{\rho}$ such that every term in every DNF in $R \restriction \rho$ mentions at most s pigeons.

Proof of Claim 1: Call a term *long* if it mentions more than $p := 2s\log(n)$ pigeons, and *short* otherwise. By Lemma 9, a long term T does not restrict to 0 (under $\boldsymbol{\rho}$) with probability at most

$$\left(\frac{1}{2} + \frac{t}{m-p}\right)^p \leq \frac{1}{2^p} \cdot e^{\frac{tp}{2(m-p)}}.$$

But this is smaller than $n^{-s} \cdot 1/2$ noting $\frac{tp}{2(m-p)} \approx 0$ for large enough n. By the union bound, with probability bigger than $1/2$ every long term of R restricts under $\boldsymbol{\rho}$ to 0.

By Lemma 10, a short term restricts to one mentioning more than s many pigeons with probability at most

$$\binom{p}{s+1} \cdot \left(\frac{t}{m}\right)^{s+1} \leq \left(\frac{pt}{m}\right)^{s+1}.$$

But this is smaller than $n^{-s} \cdot 1/2$ for sufficiently large n. By the union bound, with probability bigger than $1/2$ every short term of R restricts to one mentioning at most s pigeons. The claim follows. $\dashv$

Choose ρ according Claim 1. We already observed in Section IV-A that, up to some renaming of pigeons, $R \restriction \rho$ is a DNF-refutation of PHP^t_n of size at most n^s.

Set

$$b := 1,\ q := \lceil \sqrt{n} \rceil,\ r := \lceil n/\log n \rceil,$$
$$d_L := \lceil \log n \rceil,\ d_R := 7\lceil \log n \rceil.$$

Recall for later use that $\ell := |d_L - 1|$ and therefore ℓ is $O(\log\log n)$. Assuming n is sufficiently large the hypotheses of Lemmas 6 and 8 are satisfied for $\varepsilon := 1/2$ and imply the existence of a (U, V, d_L, d_R)-graph G that is a (q, b, r)-resilient expander where $U = [t]$ and $V = [n]$.

Recall the restriction θ_G from Section IV-B. There we observed that $PHP^t_n \restriction \theta_G$ is $PHP(G)$, so $(R \restriction \rho) \restriction \theta_G$ is a refutation of $PHP(G)$ of size at most n^s. Let ϕ_G be a map associated with G as in Section II-A. All over the refutation substitute the variable $P_{u,v}$ by the ℓ-term $\bigwedge_{b\in[\ell]} \neg^{1-\mathrm{bit}(b,j)} P_{u;b}$, where j is such that $\phi_G(u, j) = v$. Of course, the result is again a refutation. By the discussion just before Lemma 11 it refutes sporadic axioms and collision clauses of $BPHP(G)$. By Lemma 11 we can add proofs of the sporadic axioms from the domain clauses of $BPHP(G)$; this way we get a refutation R' of $BPHP(G)$ of size $n^{c_1 \cdot s}$ for some constant c_1.

Every term in every DNF in $(R \restriction \rho) \restriction \theta_G$ mentions at most s pigeons and becomes after the substitution an ℓ-CNF mentioning at most s pigeons. The additional proofs added for the sporadic axioms mention only one pigeon. Hence, R' is a refutation of $BPHP(G)$ all of whose formulas are disjunctions of ℓ-CNFs each mentioning at most s pigeons. Applying Lemma 13 we move to a refutation R'' of size $n^{c_2 \cdot s}$ for some constant c_2, where additionally all these ℓ-CNFs are matching-satisfiable.

For the next claim, let $\mathbf{B}$ and $\boldsymbol{\mu}$ be random variables defined for G as in Section IV-C.

Claim 2. There exists a realization (B, μ) of $(\mathbf{B}, \boldsymbol{\mu})$ such that

(a) $h(F \restriction \mu) \leq \frac{1}{3}\lfloor qb/d_L \rfloor$ for all F in R'', and

(b) $G \setminus B$ is a $(q, 1)$-expander.

Proof of Claim 2. Note a random $\mathbf{B}$ satisfies (b) with probability bigger than $1/2$ because G is (q, b, r)-resilient. Hence it suffices to show that for any disjunction F of matching-satisfiable ℓ-CNFs each mentioning at most s pigeons

$$n^{c_2 \cdot s} \cdot \mathbb{P}[\ h(F \restriction \boldsymbol{\mu}) > \tfrac{1}{3}\lfloor qb/d_L \rfloor\ ] \leq \tfrac{1}{2}. \qquad (6)$$

A matching-satisfiable ℓ-CNF mentioning at most s pigeons is logically equivalent to a DNF with matching-satisfiable terms each mentioning at most s pigeons. Since there are at most $s \cdot \ell$ binary pigeon variables mentioning some fixed set of $\lfloor s \rfloor$ pigeons, this DNF can be chosen as an $\lfloor s \cdot \ell \rfloor$-DNF. Thus, a formula F as above is logically equivalent to a $\lfloor s \cdot \ell \rfloor$-DNF F' where each term mentions at most s pigeons and is matching-satisfiable. In (6) we can equivalently replace F by F' (thanks to our weaker notion of representation – cf. Remark 3).

To bound the probability in (6) we intend to apply Lemma 15. By Lemmas 12 and 14, the random restriction $\boldsymbol{\mu}$ satisfies the assumptions of Lemma 15 with

$$k := \lfloor s \cdot \ell \rfloor,\ h := \lfloor \tfrac{1}{3} qb/d_L \rfloor,\ c := \lceil 3\sqrt{r} \rceil,$$

and

$$\gamma := \left(\frac{r}{d_R \cdot n}\right)^s \cdot \left(1 - \frac{r}{n}\right)^{d_L \cdot s} \cdot \frac{\log(e)}{\ell \cdot k \cdot d_L \cdot d_R}.$$

By Lemma 15 we have $\mathbb{P}[\ h(F \restriction \boldsymbol{\mu}) > \frac{1}{3}\lfloor qb/d_L \rfloor\ ]$ is at most $c \cdot k \cdot 2^{-(\gamma/4)^k \cdot h}$. Note that if n is sufficiently large, then $(1 - r/n)^{d_L \cdot s} \geq (1/e)^{c_3 \cdot s}$ for some constant $c_3 > 0$. It is then easy to see that $\gamma/4 \geq (1/\log n)^{c_4 \cdot s}$, and hence $(\gamma/4)^k \geq (1/\log n)^{c_4 \cdot s^2 \cdot \ell} \geq n^{-1/(\log n)^\epsilon}$ for some other constant $c_4 > 0$. As $h \geq n^{1/3}$ we get $(\gamma/4)^k \cdot h \geq n^{1/4}$ for sufficiently large n. Noting $c \cdot k \leq n$, then (6) follows. $\dashv$

Choose (B, μ) according to Claim 2, say, μ is associated with the matching M of G. Recall that R'' refutes $BPHP(G)$. We claim $R'' \restriction \mu$ is a refutation of $BPHP(G')$ for

$$G' := G \setminus (\mathrm{Dom}(M) \cup \mathrm{Im}(M)).$$

We have to show that every clause C of $BPHP(G)$ restricts under μ to 1 or to a clause of $BPHP(G')$. If C does not mention a pigeon in $\mathrm{Dom}(M)$, then C is a clause of $BPHP(G')$ and $C \restriction \mu = C$. If C mentions only pigeons in $\mathrm{Dom}(M)$, then $C \restriction \mu = 1$. Finally, assume C is a collision clause for $(u, j) \in \mathrm{Dom}(\phi_G)$ and $(u', j') \in \mathrm{Dom}(\phi_G)$ with $u \neq u'$ and $\phi_G(u, j) = \phi_G(u', j')$, and exactly one pigeon, say u, in $\mathrm{Dom}(M)$. If j is such that $\phi_G(u, j) \neq M(u)$, then $C \restriction \mu = 1$; otherwise,

$C \restriction \mu = \bigvee_{b\in[\ell]} \neg^{\mathrm{bit}(b,j')} P_{u';b}$ and this is a domain clause of $\mathit{BPHP}(G')$: note $\phi_G(u,j) = \phi_G(u',j') = M(u) \in \mathrm{Im}(M)$, so $(u',j') \notin \mathrm{Dom}(\phi_{G'})$. This is ensured by definition of the map associated to a restricted graph (see Section II-A).

Since $\mathrm{Im}(M) \subseteq B$, Claim 2 (b) implies that G' is a $(q,1)$-expander. Hence $R'' \restriction \mu$ contradicts Lemma 18 by Claim 2 (a).

Acknowledgements: The first and third authors would like to thank the CICYT for its support through projects TIN2010-20967-C04-04 (TASSAT) and TIN2007-66523 (FORMALISM) respectively. The second author would like to thank the FWF (Austrian Science Fund) for its support through Project P 24654 N25.

REFERENCES

[1] S. A. Cook, R. A. Reckhow. The Relative Efficiency of Propositional Proof Systems. Journal of Symbolic Logic 44(1):36-50, 1979.

[2] A. Haken. The intractability of resolution. Theoretical Computer Science 39(2-3):297-308, 1985.

[3] M. Ajtai. The complexity of the pigeonhole principle. Proceedings of the 29th Annual Symposium on the Foundations of Computer Science (FOCS), 346-355, 1988.

[4] P. Beame, R. Impagliazzo and T. Pitassi. Exponential lower bounds for the pigeonhole principle. Computational complexity 3(2):97-140, 1993.

[5] J. Krajíček, P. Pudlák and A. Woods. An exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. Random Structures & Algorithms 7(1):15-39, 1995.

[6] S. R. Buss. Polynomial size proofs of the propositional pigeonhole principle. Journal of Symbolic Logic 52(4):916-927, 1987.

[7] M. Ajtai. Approximate counting with uniform constant-depth circuits. In Advances in computational complexity theory, DIMACS Series in Discrete Mathematics and Theoretical Computer Science 13:1-20, 1993.

[8] J.B. Paris, A.J. Wilkie and A.R. Woods. Provability of the pigeonhole principle and the existence of infinitely many primes. Journal of Symbolic Logic 53(4):1235-1244, 1988.

[9] R. Raz. Resolution lower bounds for the weak pigeonhole principle. Journal of the ACM 51(2): 115-138, 2004.

[10] A. A. Razborov. Resolution lower bounds for the weak functional pigeonhole principle. Theoretical Computer Science 1(303): 233-243, 2003.

[11] A. Atserias, M.L. Bonet and J.L. Esteban. Lower bounds for the weak pigeonhole principle and random formulas beyond resolution, Information and Computation 176(2):136-152, 2002.

[12] N. Segerlind, S. Buss and R. Impagliazzo. A switching lemma for small restrictions and lower bounds for k-DNF resolution. SIAM Journal on Computing 33(5): 1171-1200, 2004.

[13] A. A. Razborov. Pseudorandom Generators Hard for k-DNF Resolution and Polynomial Calculus. Unpublished, 2003.

[14] A. Atserias. Improved Bounds on the Weak Pigeonhole Principle and Infinitely Many Primes from Weaker Axioms, Theoretical Computer Science 295(1-3): 27-39, 2003.

[15] J. Krajíček. Bounded Arithmetic, Propositional Logic, and Complexity Theory. Encyclopedia of Mathematics and its Applications 60, Cambridge University Press, 1995.

[16] J. Krajíček. On the weak pigeonhole principle. Fundamenta Mathematicae, Vol.170(1-3):123-140, 2001.

[17] A. Maciel, T. Pitassi and A. R. Woods. A new proof of the weak pigeonhole principle. Journal of Computer and System Sciences 64(4):843-872, 2002.

[18] S. Dantchev and S. Riis. On relativisation and complexity gap for resolution-based proof systems. Proceedings of 17th Annual Conference of the European Association for Computer Science Logic (CSL), Lecture Notes in Computer Science 2803:142-154, Springer, 2003.

[19] M. Furst, J. B. Saxe and M. Sipser. Parity, circuits, and the polynomial-time hierarchy. Theory of Computing Systems 17(1):13-27, 1984.

[20] E. Ben-Sasson and A. Wigderson. Short proofs are narrow – resolution made simple. Journal of the ACM 48(2):149-169, 2001.

[21] N. Segerlind. The complexity of propositional proofs. The Bulletin of Symbolic Logic 13(4):417-481, 2007.

[22] H. Robbins. A remark on Stirling's formula. The American Mathematical Monthly 62(1):26-29, 1955.

[23] B. Bollobás. Random Graphs. 2nd edition, Cambridge University Press, 2001.

[24] E. Ben-Sasson and N. Galesi. Space complexity of random formulae in resolution. Random Structures and Algorithms 23(1):92-109, 2003.

[25] A. Atserias. On sufficient conditions for unsatisfiability of random formulas. Journal of the ACM 51(2): 281-311, 2004.

[26] P. Pudlák. Proofs as games. American Mathematical Monthly, pp. 541-550, 2000.